FINDINGS

Los Alamos National Laboratory

Safeguards and Security survey

July 23 – August 9, 2001

Topical Area: INFORMATION SECURITY

Subtopic: Classified Matter Protection and Control

Inspector's Finding No.:

Report Finding No.: 01AUG09-AL-123-SSPS-IS.2-001

Finding: LANL was not marking all classified material with the classification level and classification category in accordance with DOE requirements.

Reference: DOE Manual 471.2-1B, II.3.c.(4) and d.(3)

Order requirement: Classified matter shall have classification level stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device.

Background: At the time of the survey there were approximately 53,000 classified parts at LANL, with approximately 75 percent classified at the Confidential level and 25 percent classified at the Secret level. Over 65 percent of these parts are stored in two locations – TA-41 and TA-22. A review was made of the marking and sanitization of parts. Improper marking of classified parts was noted in several locations. For instance, at one location, parts were marked as Confidential Restricted Data (CRD) and National Security Information, when in fact written correspondence stated that the parts were unclassified. At another location, placards noting that the contents of the boxes were CRD were not placed on the exterior of the box. At TA-41, hundreds of classified parts were found that were not marked with the level or type of classified information. It should be noted that these parts were stored in a vault and had been recently inventoried by the custodian. Additionally, LANL is in the process of moving the classified parts from this location to other locations which should start sometime in January 2002.

IMPACT STATEMENT: LOW. These parts are stored in a true vault in TA-41. Access to this vault is limited. LANL is in the process of moving all classified parts to other locations. The level and category of classified information needs to be identified for all classified parts – especially prior to being moved to another location.

Survey Team Member: Maggie Wood **Date:** 07/31/01

DOE/AL Team Leader: Gary Wisdom **Date:** 07/31/01

Site Representative who was present when statement of fact was validated:

Billy Pearl **Date:** 07/31/01

Topical Area: INFORMATION SECURITY

Subtopic: Classified AISS

Inspector's Finding No.: CCS-1

Report Finding No.: 01AUG09-AL-123-SSPS-IS.4-001

Finding: There was no process in place for the ISSM to be notified that managers, ISSOs, and OCSRs had completed required annual training.

Reference: PL 100-235, Sec. 5: DOE Order 471.2A, I. 9.e.(3).(e).1

Order requirement: Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system.

Background: Training for information systems security officers (ISSOs) was conducted in April 2001; however, there is no information regarding how many ISSOs did not attend the training; managers were trained in June 2001, but records do not reflect who attended the training and who did not. Organization computer security representative (OCSR) training is available on-line, yet there is no information being provided to the ISSM regarding which OCSRs have completed the training and passed the required test, nor is there any indication that the OCSR training course is added to an individual's Employee Development System training plan as mandatory annual training.

IMPACT STATEMENT: HIGH. Because the personnel who are responsible for security are required to train the users and managers in their organizations, if the security personnel are not properly trained, there is little assurance that all required protections and controls have been properly implemented.

Survey Team Member: Sue Flores **Date:** 07/27/01

DOE/AL Team Leader: Gary Wisdom **Date:** 07/27/01

Site Representative who was present when statement of fact was validated:

John Carson/Gordon Besson **Date:** 07/27/01

Topical Area:	INFORMATION SECURITY
Subtopic:	Classified AISS
Inspector's Finding No.:	CCS-2
Report Finding No.:	01AUG09-AL-123-SSPS-IS.4-002
Finding:	Policies and procedures were not updated in a timely manner.
Reference:	DOE Manual 5639.6A-1, IX.1; X.1.; and Attachment IX-2, Introduction

Order requirement: The ISSM shall ensure the development of site procedures to implement the classified AISS program.

Background: The Cyber Security Handbook is the primary reference document that is used at LANL to provide program requirements for users of classified systems. The handbook, although available on-line, has not been maintained, and contains conflicting, contradictory, and outdated information. In addition, program documentation referenced in the handbook also contains conflicting and contradictory information, and does not reflect current program requirements.

IMPACT STATEMENT: HIGH. If accurate information is not provided to all users, there is a potential for inadequate protections to be applied, and a potential for compromise of classified information.

Survey Team Member:	Sue Flores	**Date:** 07/27/01
DOE/AL Team Leader:	Gary Wisdom	**Date:** 07/27/01

Site Representative who was present when statement of fact was validated:

John Carson/Gordon Besson **Date:** 07/27/01

Topical Area: INFORMATION SECURITY

Subtopic: Classified AISS

Inspector's Finding No.: CCS-3

Report Finding No.: 01AUG09-AL-123-SSPS-IS.4-003

Finding: A current Disaster Recovery Plan was not available in the CCF.

Reference: DOE Manual 5639.6A-1, I.9.f.

Order requirement: Procedures shall be established to assure that all necessary documentation is maintained and available for continuity of operations and for disaster recovery.

Background: Interviews with the operators assigned to the Central Computing Facility (CCF) revealed that the location of the Disaster Recovery Plan for the CCF could not be determined. When a plan was found, it was dated 1997, and did not contain the names and phone numbers of current responsible personnel.

IMPACT STATEMENT: MEDIUM. The correct procedures must be followed, should there be a situation in the CCF which requires implementation of the Disaster Recovery Plan. In addition, correct identification must be noted of responsible personnel. Incorrect information delays reporting and responding to disasters.

Survey Team Member: Sue Flores **Date:** 07/25/01

DOE/AL Team Leader: Gary Wisdom **Date:** 07/25/01

Site Representative who was present when statement of fact was validated:

John Carson/Gordon Besson **Date:** 07/25/01

Topical Area: INFORMATION SECURITY

Subtopic: Classified AISS

Inspector's Finding No.: TEMPEST.001

Report Finding No.: 01AUG09-AL-123-SSPS-IS.4-004

2 Partial credit

Finding: There was no documentation that all annual TEMPEST threat assessments and special review were conducted.

5 out of 7 Ann'l Reviews

Reference: DOE Manual 200.1-1, 7.1.

Order requirement: Each TEMPESTS coordinator shall conduct a TEMPEST threat assessment and special review annually to ascertain if the TEMPEST posture has changed.

Background: Review of TEMPEST Plans and the transmission security criteria memorandum failed to disclose any record of an annual review of facilities. The TEMPEST Plans for the sensitive compartmented information facilities (SCIFs), dated 1999, were resubmitted in 2001. Attached to these plans were updated/revised threat assessments and special reviews. Review of TEMPEST Plans for non-SCIFs failed to disclose any action regarding annual assessment or reviews since the original submittal in December 1999. Of seven plans requiring annual updates, only two had the requisite assessments and reviews.

IMPACT STATEMENT: MEDIUM. The TEMPEST threat assessment and special review are the basis for all TEMPEST countermeasures and protections afforded to a facility. Annual review of the facility ensures that appropriate protections are in place.

Survey Team Member: Gary Jantz **Date:** 07/30/01

DOE/AL Team Leader: Gary Wisdom **Date:** 07/30/01

Site Representative who was present when statement of fact was validated:

D. Maes/D. Cornely **Date:** 07/30/01

Topical Area: INFORMATION SECURITY

Subtopic: Unclassified AISS

Inspector's Finding No.: UCS-1

Report Finding No.: 01AUG09-AL-123-SSPS-IS.7-001

Finding: Security features of BRASS and LAICS were not tested prior to the application being accredited.

Reference: OMB Circular A-130, Appendix III, 3.b.2).e).

Order requirement: Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application.

Background: Security features must be tested for the accrediting authority (the information systems security site manager [ISSM]) to be assured that all required controls are in place and functioning.

IMPACT STATEMENT: HIGH. If security features are not tested, there is no assurance that protection mechanisms are functioning as expected.

Survey Team Member: Sue Flores **Date:** 07/25/01

DOE/AL Team Leader: Gary Wisdom **Date:** 07/25/01

Site Representative who was present when statement of fact was validated:

John Carson/Gordon Besson **Date:** 07/25/01

151

Topical Area: INFORMATION SECURITY

Subtopic: Unclassified AISS

Inspector's Finding No.: UCS-2

Report Finding No.: 01AUG09-AL-123-SSPS-IS.7-002

Finding: Contingency plans for major applications had not been tested as required.

Reference: OMB Circular A-130, Appendix III, 3.b.2).d).

Order requirement: Establish and periodically test the capability to perform the function supported by the application in the event of failure of its automated support.

Background: The major unclassified applications at LANL, Basic Rapid Alarm Security System (BRASS) and Los Alamos Integrated Communication System (LAICS), both have accreditations based on approved security plans. Those plans state that tests will be conducted of the contingency plans for the systems on an annual basis. The contingency plan for BRASS was last tested in January 2000; no test has been conducted for LAICS.

IMPACT STATEMENT: MEDIUM. There is little assurance that BRASS or LAICS could recover from a catastrophic loss if the contingency plans are not tested.

Survey Team Member: Sue Flores **Date:** 07/25/01

DOE/AL Team Leader: Gary Wisdom **Date:** 07/25/01

Site Representative who was present when statement of fact was validated:

John Carson/Gordon Besson **Date:** 07/25/01

Topical Area: INFORMATION SECURITY

Subtopic: Unclassified AISS

Inspector's Finding No.: UCS-3

Report Finding No.: 01AUG09-AL-123-SSPS-IS.7-003

Finding: The Protection Program Plan (PPP) does not accurately describe required protections for unclassified information.

Reference: OMB Circular A-130, Appendix III, 3.

Order requirement: Each program shall implement policies, standards, and procedures which are consistent with government-wide policies, standards, and procedures.

Background: The Protection Program Plan is the "umbrella" plan which describes the standards of protection for unclassified information at LANL. It also references other LANL program documents (cyber security handbook, Information Architecture standards, etc.) which give conflicting or inaccurate information on program requirements.

IMPACT STATEMENT: HIGH. The PPP is the major source of program requirements for LANL personnel. If accurate information is not provided, there is little assurance that information is protected in a consistent manner.

Survey Team Member: Sue Flores **Date:** 07/27/01

DOE/AL Team Leader: Gary Wisdom **Date:** 07/27/01

Site Representative who was present when statement of fact was validated:

John Carson/Gordon Besson **Date:** 07/27/01

Facility: LANL

Topical Area (*circle one*): PM PPO [✓ IS] NMC&A PS

Subtopic: Protected Transmission Systems

Inspector's Finding No.: PTS-001 *Classification:* [✓ U] C S *Level:* NSI RD

Report Finding No. (*to be provided by editor*): ______

Finding: **Formal, documented inspections of inaccessible, aerial and unexposed classified distributive information network runs are not conducted.**

Reference: DOE Order DOE Manual 200.1-1 **Chapter** 5 **Paragraph** 4.8
(or other Doe requirement)
DOE Manual as amended

Order Requirement (*verbatim, if possible*):

Inaccessible, Aerial or Unexposed CDIN must receive an initial technical inspection and a visual inspection annually thereafter.

Background (*include all pertinent information related to finding*):

Discussions with the LANL PTS Site Manager and review of relevant records disclosed that no formal inspection process exists for inaccessible, aerial or unexposed CDIN. The PTS Site Manager does not maintain a listing of locations where this type of CDIN has been installed. Furthermore, the Site Manager was not aware of this annual requirement. These runs would be visually inspected during any modification to the run, during the biennial inspection program, or through casual observation by the PTS Site Manager or by members of the protective force during routine patrols.

IMPACT STATEMENT (*describe what could happen if finding is not corrected*) [✓ LOW], MEDIUM, OR HIGH (*Circle one.*): The possibility exists that a modification could be made to the CDIN, providing for unauthorized access to classified information through wiretapping. This is partially offset by Cyber Security protocols and protections. Detection of the wiretap should occur during the next inspection, sometime during a two-year period.

Survey Team Member: G. Jantz **Date:** 7/31/01

Survey Team Leader: G. Wisdom **Date:** 7/31/01

Site Representative who was present when statement of fact was validated:

Name: R. Roybal **Date:** 7/31/01

RATINGS

Los Alamos National Laboratory

Safeguards and Security survey

July 23 – August 9, 2001

155

LANL 08/09/01

DOE Form (F) 5634.1 (5-94)

U.S. DEPARTMENT OF ENERGY
SAFEGUARDS AND SECURITY SURVEY REPORT

(This page contains no classified information)

OMB Burden Disclosure Statement

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, researching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information, Resources Management Policy, Plans, and Oversight, Records Management Division, HR-422, - GTN, Paperwork Reduction Project (1910-1800), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-1800), Washington, DC 20503.

1. Survey Type: □ Initial ■ Periodic □ Special □ Termination		2. Report #: 01AUG09-AL-123-SPPS
3. Facility Name: Regents of the University of California dba Los Alamos National Laboratory		4. A. Facility Code: 123 B. RIS Code: AUA, VUA
5. Survey Date(s): July 23 - August 9, 2001	6. Findings: ■ Yes □ No	7. Composite Rating: SATISFACTORY
8. Previous Survey Date(s): September 11-15, 2000	9. Unresolved Findings: ■ Yes □ No	10. Previous Rating: MARGINAL

11. Ratings:

A) PROGRAM MANAGEMENT

Program Management and Administration	S
Program Planning	S
Personnel Development and Training	S
Facility Approval and Registration of Activities	S
Foreign Ownership, Control, or Influence	S
Safeguards and Security Plans	S
Surveys and Self Assessment	S
Resolution of Findings	S
Incident Reporting and Management	S
OVERALL RATING	S

B) PROTECTION PROGRAM OPERATIONS

Physical Security	S
Security Systems	S
Protective Force	S
Security Badges, Credentials, and Shields	S
Transportation Security	S
OVERALL RATING	S

C) INFORMATION SECURITY

Classification Guidance	DNA
Classified Matter Protection and Control	S
Special Access Programs and Intelligence Information	S
Classified Automated Information Systems Security	M
Technical Surveillance Countermeasures	S
Operations Security	S
Unclassified AISS (Optional)	M
Protected Distribution System (Optional)	S
Communications Security (COMSEC) (Optional)	S
OVERALL RATING	S

D) NUCLEAR MATERIALS CONTROL AND ACCOUNTABILITY

Basic Requirements	S
Material Accounting	S
Material Control	S
OVERALL RATING	S

E) PERSONNEL SECURITY

Access Authorization (Personnel Clearance)	S
Security Education Briefings and Awareness	S
Control of Visits	S
Unclassified Visits and Assignments by Foreign Nationals	S
Personnel Assurance Program	S
Personnel Security Assurance Program	S
OVERALL RATING	S

12. Surveying Office: AL

13. Report Prepared by:
Gary D. Wisdom, Security Specialist, AAO
Date: 10/17/01

14. Report Approved by: Richard W. Phillips
Richard W. Phillips, Acting Director, Safeguards and Physical Security Division (SPSD, AL
Date: 10/22/01

15. Distribution: DP-43, HQ—1 cy; LAAO—2 cys

Rate Each Item: S = SATISFACTORY M = MARGINAL U = UNSATISFACTORY DNA = DOES NOT APPLY

Classified AISS
Rating Rationale

The classified AIS security program at LANL has suffered from a significant lack of funding, which in turn caused a severe reduction in the number of personnel assigned to manage the program. Both of these factors have contributed to the problems with program documentation and the lack of adequate training for cyber security personnel (ISSOs and OCSRs). There is a potential for classified information to be compromised, yet at this time there is no evidence that information is not protected at the minimum required levels. The information is, however, at increased risk. Should the condition continue, classified information may well be compromised. Because there is only limited assurance that the protection objectives have been met, and due to the repeat finding assessed during this survey, the subtopic "Classified AIS Security" is rated MARGINAL.

Unclassified AISS
Rating Rationale

Although there are problematic program issues, such as contradictory and/or conflicting information, and a lack of a well-defined program, there is nio evidence that unclassified information is at risk. If the inconsistencies and neglect are allowed to continue, however, there is a significant potential that sensitive information could be compromised. Because the protection objectives are only partially met, the subtopic "Unclassified AIS Security is rated MARGINAL.

INSPECTION PLANNING AND REPORTING GUIDELINES

Survey team member preparation ongoing

Team Preparation Source Documents

Master Survey Plan
Generic Individual Survey Plans
Draft survey schedule matrix development
Facility Data Card for 123, effective 09/00
DRO listing for LANL interests
SSIMS Printout
FOCI Listing (Sheehan), effective 09/01/00
Copy of PF Annual Training Plan w/approval ltr
Copies of SSSP
Copy of SSSP approval - transmittal memorandum
Copies of AL Inspection Reports (1998 and 1999)
Copy of most recent OSE Site Profile
Copies of 1999 OA inspections

Initial survey team meeting – 08/16/00
Personnel security data call due to AL – 08/21/00
Areas of special emphasis from LAAO – 08/16/00
Draft Inspection Plans – 08/28/00
Data call due – 09/11/00
Survey Team Meeting/Briefing - 09/10/00
Finalization of Inspection Plans – 09/11/00
In-briefing – 09/11/00 – 8 a.m.

Daily team meeting - 4:30 p.m.

Draft report writing complete – 5 p.m. – 09/15/00

Murder board - 09/14/00 – 2 p.m.

Working Close-out – 09/15/00 – 11 a.m.
(Location TBD)

Management Close-out - 09/26/00 – 9 a.m.
(Location TBD)

Report Transmittal - target date – 11/17/00

SAFEGUARDS & SECURITY SURVEY
LOS ALAMOS NATIONAL LABORATORY
September 11-15, 2000

INSPECTION/WRITING ASSIGNMENTS
(Revised September 8, 2000)

Team Leader – Rich Lucero
Assistant Team Leader – Frank Ward

A.	PROGRAM MANAGEMENT	Lyle Hofferth (Topic Lead)
A.1.	Program Management and Administration	"/Art Flynn/Eileen Johnston
A.2.	Program Planning	"
A.3.	Personnel Development and Training	N/A
A.4.	Facility Approval and Registration of Activities	N/A
A.5.	Foreign Ownership, Control, or Influence	N/A
A.6.	Safeguards and Security Plans	N/A
A.7.	Surveys and Self-Assessment	Eileen Johnston/Monte Mortensen
A.8.	Resolution of Findings	Judy McGurn/Lorenzo Carrillo
A.9.	Incident Reporting and Management	"
B.	PROTECTION PROGRAM OPERATIONS	Art Flynn (Topic Lead)
B.1.	Physical Security (will NOT include VTRs) Protective Lighting Physical Barriers Lock and Key Control Personnel and Vehicle Access Control Property Protection	Ronnie Pierce/John Peterson
B.2.	Security Systems	Richard Gonzales/DK (Red) Jones/Desiree Saupe
B.3.	Protective Force	Art Flynn/Doug MacKinlay/Bert Creasey/Stacy Kubasek/Monte Mortensen
B.4.	Security Badges, Credentials, and Shields	Ronnie Pierce/Lorenzo Carrillo
B.5.	Transportation Security	"
C.	INFORMATION SECURITY	Richard Keck (Topic Lead)
C.1.	Classification Guidance	N/A
C.2.	Classified Matter Protection and Control	Clarence Marquez/Richard Keck/Judy McGurn
C.3.	Special Access Programs and Intelligence Information	Lowell Little
C.4.	Classified Automated Information Systems Security	Sue Flores/Angela Scheurenbrand/Kurt Snapper
C.5.	Technical Surveillance Countermeasures	N/A
C.6.	Operations Security	N/A

C.7.	Unclassified AISS	Sue Flores/Angela Scheurenbrand/Kurt Snapper
C.8.	Protected Transmission System	N/A
C.9.	Communications Security	N/A
D.	NUCLEAR MATERIALS CONTROL AND ACCOUNTABILITY	Cindy Murdock (Topic Lead)
D.1.	Basic Requirements	Cindy Murdock/John Andrews
D.2.	Material Accountability	John Andrews/Andy Sandoval/Usha Narayanan
D.3.	Material Control	Al Garrett/Sherri Cross
E.	PERSONNEL SECURITY	Judy McGurn (Topic Lead)
E.1.	Access Authorization (Personnel Clearance)	*/Elaine Ramierz
E.2.	Security Education Briefings and Awareness	N/A
E.3.	Control of Visits	N/A
E.4.	Unclassified Visits and Assignments by Foreign Nationals	N/A
E.5.	Personnel Assurance Program	N/A
E.6.	Personnel Security Assurance Program	N/A

LANL 2000 Security Survey

Inspection Plan – Program Management and Administration

Documentation

- Organization diagrams depicting the management structure
- Documents depicting responsibilities and authorities of S&S management
- Position descriptions for S&S management positions
- Operating instructions for the implementation of S&S programs
- Supplemental Orders/Directives implementing S&S programs
- LANL contract and oversight responsibilities for PTLA contract
- SSSP defining critical S&S elements and documentation related to management and administration programs for these critical elements

Interviews

- LANL S&S Program Managers
- LANL management assigned responsibility for developing and implementing the Program Management and Administration for the S&S program
- LANL management assigned responsibility for developing and implementing the S&S programs.
- PTLA management interfacing with LANL
- LAAO management interfacing with LANL

Performance Measures

After the completion of document reviews, interviews, and observations of the day-to-day activities, the inspectors will be able to measure the effectiveness of management and administration of the S&S program. The documentation in place will be used to determine how well management requirements have been implemented, to include, for example, the lack of resources or other previously identified deficiencies have been resolved. A determination of the programmatic guidance and forecasts of significant changes planned in site operations can be identified. The current and projected operational constraints and resources shall also be identified. Other forms of measurement may also be developed to assist the survey team in determining the effectiveness of the management of the S&S programs.

Question for Program Management and Administration

Goal 1 –Are sufficient resources available to meet S&S requirements?

1. What is the S&S budget for FY 2000? FY 2001? (Break up into Line Items, Capital, Operating, etc)
2. What is LANL S&S staffing level by organization?
3. Have you request additional staffing?
4. How do you strike a balance between various goals, problems and needs?

Goal 2 – Are they managing/controlling the resources?

1. Is the organization structured properly to provide comprehensive coverage of all the S&S programs?
2. How do you assure specific tasks are done successfully?
3. Do you evaluate how well the task was accomplished?
4. How do you hold your managers accountable for their particular tasks?
5. How do you hold managers responsible for the allocation of resoures in pursuit of achieving the tasks?
6. Do you use analytical techniques to break down a problem/task into components to obtain a feasible solution?
7. Are you using technology to reduce costs?

Goal 3 – Are appropiate interfaces in place to implement a satisfactory S&S program

1. Do you meet with Senior management within LANL organizations? Frequency? Do you meet with organizations outside LANL? (DOE/AL, LAAO, PTLA, LAPD, etc)
2. What means do you use to communicate security issues/requirements to LANL organizations?
3. What means do you communicate/interact between LANL S&S managers?
4. Do you have a stakeholder diagram which shows your customers?
5. Who is the LANL S&S POC (mentor) for site reps? How often do they meet? How much time is the site rep dedicated to security? What is expected of the site rep? Does he/she have a PD?

Goal 4 – Does management have the clout/structure to get other management organizations to meet S&S requirements?

1. What relationships have you built to promote accomplishment of organizational goals? (customer service for other LANL managers, etc)
2. Do you serve as an official representative of your organization at other LANL organizational meetings? ((clients, customers, contractors, SOE official and personnel of other organizations)

Goal 5 – Is the S&S Organization highly motivated to improve security?

1. Do you hold periodic staff meetings? Frequency?

2. Do you have organizational goals? Over what periods e.g. 1,2-5yr? How are the goals monitored? What is the frequency of monitoring?

3 What methods are used to obtain accurate information to evaluate the status of your programs? (self-assessment, spot audits, etc.)

4 Do you evaluate contribution/productivity of employees?

5 Are there any formalized disputes within your organizations?

6 Have you had to be a mediator to resolve disputes as they occur?

Goal 6 – Does management have systems in place to monitor critical systems to assure adequate operation?

1. How many critical systems do you have?

2. What methods are used to obtain accurate information to evaluate the status of the critical systems?

3 How effective is the program?

4. Do you do trending? How do you determine a problem?

6. Are the monitoring of the critical elements scheduled? Who assures they are on schedule?

6. What is the number of completed versus scheduled Critical Element testings.

determine the degree of effectiveness of LANL's program planning. The documentation will be used to evaluate projected needs for funding, staffing, and upgrades to ensure an effective S&S program. The reviews conducted by the balance of the survey team will be used to determine any deficiencies in staffing/personnel and any significant programmatic deficiences that have not been addressed. In addition, the interviews will identify any constraints which would not allow LANL to obtain desired/projected resources. Other forms of measurement may also be developed to assist the survey team in determining the effective of LANL's S&S program planning.